Here is a bit of very interesting e-news.

Major topics include:
From: [hipaalert] HIPAAlert - Vol. 3, No. 1 - 1/17/02
1. From the Editors: A New HIPAAlert for 2002!
2. HIPAAnews: IT Security Update, New IDs, and the Latest on Transactions
3. HIPAAction: The New Transactions Deadline -- What It Means to You
4. HIPAA / EDI: Q/A -- What Transaction Versions Should You Implement?
5. HIPAA / Secure: Security Q/A -- Are Viruses Getting Worse?
6. HIPAA / Law: Legal Q/A -- Organized Arrangements vs. Affiliated Entities

Please be sure to note that in some cases the information presented may be the opinion of the original author. We need to be sure to view it in the context of our own organizations and environment. In some cases you may need legal opinions and/or decision documentation when interpreting the rules.

Have a great day!!!
Ken

********** [hipaalert] HIPAAlert - Vol. 3, No. 1 - 1/17/02 **********
>>> <info@phoenixhealth.com> 01/17/02 03:15PM >>>
==========

H I P A A L E R T Volume 3, Number 1 January 17, 2002

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
> Healthcare IT Consulting & Outsourcing <

==========
HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total nearly 16,000.

IF YOU LIKE HIPAALERT,YOU'LL LOVE www.HIPAADVISORY.COM! -- Phoenix'"HIPAA hub of the Internet" per Modern Healthcare.
==========

T H I S I S S U E

1. From the Editors: A New HIPAAlert for 2002!

==========

1 >> F R O M T H E E D I T O R S:

The New Year officially marks the start of HIPAAlert's third year...a fitting time, we thought, for a minor HIPAAlert "makeover." Hands-on implementation, clearly, is presenting ever more pressing issues for most of us, so this edition of HIPAAlert introduces two practical monthly Q/A columns -- one on Transactions and Code Sets and the other on Security. We are pleased to welcome two past contributors as our new monthly "regulars:" Kepa Zubeldia, President and CEO of Claredi, who is authoring HIPAA / EDI: Q/A on Transactions & Code Sets; and Eric Maiwald, CTO of Fortrex Technologies, who will author HIPAA / Secure: Security Q/A. Well-known leaders in their respective fields, both Kepa and Eric have provided notable contributions to the healthcare industry through their original research and widely read publications.

Steve Fox and Rachel Wilson of Pepper Hamilton, LLP will continue their excellent work producing incisive legal briefings on HIPAA issues in HIPAA / Law: Legal Q/A. As always, their monthly contributions -- as well as Kepa and Eric's new columns -- will be collected in their own Q/A sections of HIPAAdvisory.com for your ongoing reference.

The New Year also marked President Bush's final approval of the long discussed, often controversial Administrative Simplification Compliance Act, formerly known as HR 3323 -- and generally dubbed the "Transactions Delay Bill." Steve Fox and Rachel Wilson lead off this issue of HIPAAlert with a comprehensive analysis of the new law's deadline extension features -- sure to be of interest to anyone who has been on pins and needles wondering how the original October 2002 deadline could be met.

We'd like to know what you think of HIPAAlert -- including its new and not so new features. Please email us your comments and suggestions, and we'll be happy to respond!

D'Arcy Guerin Gue
Publisher

dgue@phoenixhealth.com

Bruce Hall
Director of Internet Services
bhall@phoenixhealth.com

==========
==========

2 >> H I P A A n e w s

*** CERT: Security Incidents More Than Double in 2001 ***

The number of security incidents reported to the Computer Emergency Response Team Coordination Center (CERT/CC) more than doubled in 2001 compared with the prior year, according to figures the group released January 11, reports ComputerWorld. Security incidents have risen nearly every year since CERT's founding in 1988. That trend has risen sharply in the past few years with nearly 10,000 incidents reported for 1999, more than 21,000 in 2000 and now nearly 53,000 in 2001. Reports of security vulnerabilities in software have followed the same trend as security incidents as well.

Read more: http://www.hipaadvisory.com/news/index.htm#0114cw

*** Congressional Comments on Transactions Extension Bill Published ***

Comments on the Administrative Simplification Compliance Act, formerly known as HR 3323, have been inserted in the Congressional Record by congressional leaders. Their discussion of the new law covers summary compliance plans, use of DHHS' model form, NCVHS analysis of compliance extension plans and other features of the law.

Read the full text of their comments at:
http://www.hipaadvisory.com/news/2001/1229tcsdelay.htm

*** Feds, Motor Vehicle Group Move Toward Driver's Licenses with High-Tech Identifiers ***

The government is taking first steps to develop driver's licenses that can electronically store information -- such as fingerprints -- for all Americans who carry the cards. Privacy experts fear that such a move could lead to de facto national identification cards that would allow authorities to track citizens electronically, and would circumvent the current debate concerning federal ID cards. The Transportation Department, under instructions from

Congress, is expected to develop rules for states to encode data onto driver's licenses to prevent criminals from using them as false identification.

State motor vehicle officials planned to ask Congress this week for up to $100 million to create a national ID system that would include high-tech driver's licenses and a network of tightly linked databases of driver information. Officials from the American Association of Motor Vehicle Administrators want cards containing fingerprints, computer chips or other unique identifiers to improve security. "Driver's licenses," they say, "have already become the de facto national identification card."

Read more: http://www.hipaadvisory.com/news/2002/0110natlid.htm

*** VIRUS ALERT: JS.Gigger Worm Spreading ***

Multiple sources confirm the spread of a new Internet worm. JS.Gigger.A@mm, a worm written in JavaScript, uses Microsoft Outlook and mIRC to spread itself, like many other recent worms and viruses. It attempts to delete all files on the computer and to format drive C if the computer is successfully restarted. The worm arrives as an email message that has the following characteristics:

Subject: Outlook Express Update
Message: MSNSofware Co.
Attachment: Mmsn_offline.htm

Technical information:
http://www.symantec.com/avcenter/venc/data/js.gigger.a@mm.html

==========

3 >> H I P A A c t i o n: Feature Article

"The New Transactions Compliance Extension: What It Means to You"

By Steve Fox, Esq., Partner, and Rachel Wilson, Esq., Pepper Hamilton LLP

The compliance date for HIPAA's Electronic Transaction Standards has been delayed. Well, sort of. President Bush recently signed the "Administrative Simplification Compliance Act," providing a one-year extension of the compliance date to covered entities that submit a plan describing how they will achieve compliance by the extended October 16, 2003 deadline. (Note: this is the same deadline which previously applied only to small health plans, and remains unchanged by this legislation.)

The required compliance plans must be submitted to HHS no later than October 16, 2002 -- the original compliance date. Plans must summarize the following:

1. An analysis reflecting the extent to which, and the reasons why, the entity is not in compliance;
2. A budget, schedule, work plan, and implementation strategy for achieving compliance;
3. Whether the entity plans to use or might use a contractor or other vendor to assist the entity in achieving compliance; and
4. A timeframe for testing that begins not later than April 16, 2003.

It is important to note that this date falls only SIX months after the original compliance deadline. In order to be ready for testing by this date, covered entities will have to make significant progress over the next year towards completion of their implementation/conversion plans.

On its end, HHS is required to publish a model compliance plan form by March 31, 2002. Covered entities may utilize the HHS form to submit the mandated information, or may use an alternative format.

What Was Congress' Intent?

This new law represents Congress' attempt to balance its concerns about delaying compliance against the legitimate reasons why compliance by October 2002 is untenable for many organizations. An unconditional one year delay had the potential to yield to indefinite extensions, falling prey to status quo advocates who would present new excuses and request additional extensions. Consequently, including the compliance plan requirement is intended to force covered entities to focus on implementation efforts and help them map out the exact steps needed to ensure compliance.

One of the underlying goals of Congress' compliance plan requirement is to support implementation efforts. Accordingly, the plans are not subject to HHS approval, but instead will be used to assist covered entities with their compliance initiatives. A sampling of the plans will be distributed to the National Committee on Vital and Health Statistics (the "NCVHS"), which intends to publish reports offering effective solutions to compliance problems identified in the submitted compliance plans. The reports will not focus on any one plan, but will be generalized and address the most common or challenging problems identified in the plans submitted. Confidential information included in compliance plans will be removed prior to NCVHS' publication of reports.

Will the Act Be Enforced?

In a word, yes. Covered entities that fail to submit compliance plans are required to comply with the electronic transaction standards no later than the original deadline of October 16, 2002. Organizations that fail to submit a compliance plan or implement the transaction standards by then may face exclusion from participation in Medicare, in addition to any and all other penalties permissible under HIPAA.

What About the Privacy Rule Deadline?

The Act specifically notes that its provisions do not affect the April 2003 compliance date for HIPAA's Privacy Standards. Congress wanted to ensure that entities comply with the Privacy Standard despite the fact that they may not be subject to the Transaction Standards until six months after the Privacy Standard goes into effect. Toward that end, covered entities are required to protect the confidentiality of patient information regardless of whether the data is transmitted in the format mandated under the Electronic Transaction Standards.

Can't We Just Go Back to Paper Claims?

In line with HIPAA's goal to promote industry-wide use of electronic transactions, the Act provides a strong disincentive to those considering a return to paper claims management. Covered entities are prohibited from submitting paper claims to Medicare after October 16, 2003. Submission of electronic, HIPAA compliant, Medicare claims will be a condition of payment from that date forward. There are waivers for certain small providers or if there is no method for electronic submission of claims available. Further details about this requirement are forthcoming.

The Act also expressly includes the Medicare+Choice program under the definition of a health plan, making these organizations covered entities and requiring them to comply with HIPAA as well.

Pepper Hamilton, LLP is a multi-practice law firm with more than 425 lawyers in 11 offices. Steve Fox leads Pepper's healthcare informatics practice.
http://www.pepperlaw.com

==========

4 >> H I P A A / EDI: Q/A on Transactions & Code Sets
>> by Kepa Zubeldia, M.D., President and CEO, Claredi

"What Transaction Versions Should You Implement?"

QUESTION: Which standard transactions should we implement, the May 2000 version or the October 2001 Addenda version?

ANSWER: Since the publication of the Transaction "Addenda", this question has been a recurring theme in my email. The answer, as usual, is a definite "it depends". Now that the Administrative Simplification Compliance Act (ASCA) has been signed into law, and covered entities are allowed some extra time for compliance, the "it depends" answer becomes easier to understand. :-)

Let me explain, starting with a little history...

Under HIPAA, the Secretary of HHS is allowed to change the transactions standards only once per year. And, whenever there is a change, the Secretary must allow at least 6 months to implement the changes.

But, there is one exception. During the first year after adoption of any standards, the Secretary can change the standards "if necessary for implementation". After that initial course correction, the changes must be spaced at least one year apart.

As it turns out, as soon as the May 2000 Implementation Guides (IGs) were published, the authors began finding errors in them. Some were minor typographical errors. Some were confusing, incomplete, or conflicting instructions. Still others were major course corrections, such as removing the requirement for provider taxonomy codes. Within just a few months, nearly two hundred "problems" were identified in the IGs. And some were the kind where correction was "necessary for implementation."

The Designated Standards Maintenance Organizations (DSMOs) went to work on these issues and, after some grueling sessions, agreed on solutions to issues that were "necessary for implementation." The IGs were revised by X12N, and thus the "Addenda" to the implementation guides were born.

Some of the Addenda barely change the guides. For example, the 820 transaction Addendum changes only the version number and adds one note. Most have just a few changes. The 278 Referral Addendum, however, is 218 pages long. But some of the changes in the Addenda are related to "situational" requirements that may not affect you at all.

The important thing to remember is that the Addenda were produced to facilitate the implementation of the transactions. And they do a good job at that. It is easier to implement the Addenda versions than the May 2000 version of these IGs. That was the whole point of having Addenda -- to make the implementation easier and, in some cases, to make the implementation even possible.

The Addenda still are not quite final. But any changes will probably be minor, since they have had extensive review and are the result of a true industry consensus. For this reason it's likely that the Addenda will be published soon, through the required "Notice of Proposed Rulemaking"

(NPRM). Following 30 days for public comment and any final tweaking, the Addenda will be formally adopted by HHS as a Final Rule.

So, which version should you implement? It depends...

If you are one of the few providers not affected by changes in the Addenda, and you are almost complete with your development of the May 2000 version, and you and your payers expect to be ready to exchange May 2000 version transactions before October 16, 2002, you may want to proceed on this course. Then, to get ready for the rest of the HIPAA world, start working on the Addenda version as soon as the Final Rule comes out. Or sooner.

But, if the Addenda make your implementation easier, or you want to implement only one version of each guide, then you need to look at the Addenda soon. Keep in mind that implementing the Addenda will require a new gap analysis and some programming changes. Most changes in the Addenda are not too drastic, so the work to migrate from the May 2000 IGs to the Addenda version will seem like "pedaling down hill." Still, there is some work involved.

It's important to recognize that there is no "end" to HIPAA transaction standardization...it is an evolving process. In the future there will be new versions of the IGs, new transactions, and new opportunities for EDI based benefits. The Addenda is the first step in this evolution.

Hopefully, future steps down this road will continue the trend of making Administrative Simplification even "simpler" to achieve.

==========

5 >> H I P A A / SECURE: Security Q/A
>> by Eric Maiwald, CISSP, Chief Technology Officer, Fortrex Technologies, Inc.

"Are Computer Viruses Getting Worse?"

QUESTION: Viruses seem to be getting more dangerous in the last few months. Do you expect this trend to continue and what can be done to reduce the impact on my organization?

ANSWER: Your impression is absolutely correct and yes, I would expect the trend to continue. But, before I get too far into this answer, I would like to

clear up a bit of terminology. There are actually three types of programs that we see causing problems:

* Viruses - a program that piggy backs on a legitimate program. Examples are Melissa and Michelangelo.

* Worms - a program that executes on its own and uses its own code to spread. Examples are Code Red and SaAdmind.

* Trojan Horses - a program that pretends to be something it is not. Examples are Anna Kournikova and ILOVEYOU.

Collectively these programs are called "malicious code." We are also beginning to see programs that exhibit characteristics of multiple categories. For example, Nimbda had characteristics of both a worm and a Trojan horse in that it spread by attacking web servers as well as by tricking users into opening an email attachment.

In the last few months we have seen these programs get more sophisticated and much more dangerous. For example, the Code Red worm damaged hundreds of thousands of systems in a very short time. The two most interesting programs (as far as sophistication and potential damage) are BadTrans, which captured keystrokes on user computers, and Goner, which disabled anti-virus software. Clearly, if we begin to see more programs like this, the potential for damage (especially loss of time and resources) is very high.

How can you reduce the impact of these programs on your organization? There are five primary tactics that together provide reasonable protection for your organization:

1. Use anti-virus software and keep the signatures updated. Keep in mind that signatures can come out very quickly in response to a new virus or worm and thus you should check for updates daily. Having the program automatically check for and then push out these updates helps a lot.

2. Check incoming and outgoing emails for malicious programs. There are a number of software packages that will check email attachments for worms and viruses as the mail comes into or goes out of the organization. These can prevent the initial infection even if the users don't update their signatures. Of course, this type of system does require the administrators to keep the email checking programs up to date.

3. Teach your users about malicious programs. The most important link in preventing viruses and Trojan horses is the user. The user must understand what not to do. They should know not to open attachments that they are not expecting.

4. Set up proper access control inbound and outbound through your firewalls. If rules are properly configured on your firewall, many worms can be prevented from spreading. For example, do not allow your web server to open outbound connections. This would prevent Code Red from spreading if your web server were infected.

5. Patch your systems to prevent vulnerabilities from being exploited. Some of the more recent worms are using new vulnerabilities in servers to spread. Keep the systems patched and you will reduce the likelihood that they will be successfully attacked.

Fortrex Technologies, a Phoenix Health Systems security partner, provides enterprise security management services and information security process and monitoring services for healthcare and other industries.
http://www.fortrex.com

==========

6 >> H I P A A / LAW : Legal Q/A
>> by Steve Fox, Esq., & Rachel Wilson, Esq., Pepper Hamilton LLP

QUESTION: What is the difference between an organized health care arrangement ("OHCA") and affiliated entities?

ANSWER: There are two primary differences between affiliated covered entities and an OHCA. First, affiliated entities and an OHCA differ from one another regarding the way that information may be used or disclosed by and between the covered entities that populate them. Second, the common required element shared between the components of an affiliated entity and the participants in an OHCA are different.

Entities sharing common ownership or control may adopt the "affiliated entity" designation recognized under the Privacy Standards. For example, a corporation which owns hospitals in several different states could opt to make such an election. The designation basically functions to erase the individual identity of each separate entity and create one single covered entity for the purpose of complying with the Privacy Standards. The exception is that each component of an affiliated entity is required to erect firewalls to protect against the improper use or disclosure of protected health information ("PHI") within the affiliated entity. Because they enjoy the fiction of existence as a single entity under the Privacy Standards, affiliated entities may utilize a single consent form and notice of privacy practices.

Unlike an OHCA, discussed below, the covered functions performed by each distinct component of an affiliated entity are not required to be similar to one another or arise out of a single integrated enterprise or practice.

Forming an OHCA is generally, but not exclusively, permissible in those integrated care settings where participants need to share PHI about their patients in order to manage and benefit the common enterprise. One example would be a hospital setting where both the hospital and the physician with staff privileges provide treatment. The principal concept underlying the OHCA is the idea that in certain integrated settings, covered entities need the unrestricted right to share health information. Accordingly, the Privacy Standards permit participants in an OHCA to use and disclose PHI for the treatment, payment, and health care operations of the entire arrangement just as they would for their own such purposes. Toward that end, component entities may join together to promulgate a joint notice of privacy practices as well as a joint consent.

In general, component entities of an OHCA may share PHI for the joint management and operations of the arrangement without patient consent or authorization. This is true except where direct providers are included in the arrangement. In that event, a general consent is required before any component entity would be permitted to use or disclose PHI.

To read past HIPAA Legal Q/A articles, go to:
http://www.hipaadvisory.com/action/HIPAAdvisor.htm

Steve Fox, Esq., is a partner at the Washington, DC office of Pepper Hamilton LLP. This article was co-authored by Rachel H.Wilson, Esq., of Pepper Hamilton LLP.
http://www.pepperlaw.com/
Disclaimer: This information is general in nature and should not be relied upon as legal advice.

==========

DON'T MISS our January HIPAA audioconference!

>> Between a Rock and a Hard Place:
Assessing the Impact of the TCS Compliance Extension <<

Thursday, January 24 -- With Clyde Hewitt, Principal,
Phoenix Health Systems

For more info, or to enroll, go to:
http://www.hipaadvisory.com/ezcart/index.cfm

Other outstanding HIPAA Audioconferences and tapes available at:
http://www.hipaadvisory.com/ezcart/

==========

Phoenix Health Systems offers both text and HTML versions of HIPAAlert. To switch to HTML format, fill out the short form at:
http://www.hipaadvisory.com/signup/change.cfm
==========

BRING YOUR HIPAA QUESTIONS & IDEAS TO LIFE AT...H I P A A l i v e!

Join over 4000 other thinkers, planners, learners and lurkers who are already members of our sister e-mail discussion list. We almost make HIPAA fun! Almost. Subscribe now at: http://www.hipaadvisory.com/live/

==========

RAISE YOUR ORGANIZATION'S HIPAAWARENESS WITH H I P A A n o t e s!

8500 subscribers already receive our weekly byte of HIPAA. HIPAAnotes are suitable for publishing on your organization's intranet or newsletter & come free to your e-mailbox. Subscribe now at:
http://www.hipaadvisory.com/notes/

==========
COMMENTS? E-mail us at info@phoenixhealth.com
SUBSCRIBE? Visit http://www.hipaadvisory.com/alert/
ARCHIVES: http://www.hipaadvisory.com/alert/newsarchives.htm
==========

==========

Switch to HTML version or to text version at:
http://www.hipaadvisory.com/signup/change.cfm
======
To view the list's archives, change your settings, or unsubscribe, go to:
http://lyris.dundee.net/cgi-bin/lyris.pl?enter=hipaalert